FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of University Building Access Controls

Report No. 15/16-06

January 20, 2016

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

MEMORANDUM

DATE: January 20, 2016

TO: Kenneth A. Jessell, Senior Vice President and Chief Financial Officer
John Cal, Associate Vice President for Facilities Management

FROM: Allen Vann, Chief Audit Executive

SUBJECT: **Audit of University Building Access Controls, Report No. 15/16-06**

Pursuant to our approved annual plan, we have completed an audit of University Building Access Controls. The primary objective of our audit was to determine if policies and procedures related to building access controls were adequate and effective. This included the evaluation of controls in place to prevent unauthorized access and safeguard resources.

The University designated the Facilities Management Department as the central point for the issuance, maintenance and secured storage of all types of software, hardware and access mechanisms used on interior and exterior doorways for all campus buildings and facilities. There are 87 buildings at Modesto A. Maidique Campus containing 16,197 rooms and 18 buildings at Biscayne Bay Campus that have 2,201 rooms. At any given time, any of 54,000 students, 11,000 employees, and numerous others visit our facilities.

Overall, our audit disclosed that policies and procedures related to building access controls are inadequate. Also, controls to prevent unauthorized access, safeguard resources, and promote safety need significant improvement. This will require a significant and timely collaborative effort by cognizant officials throughout the University. The audit resulted in fourteen recommendations, which management agreed to implement.

We would like to take this opportunity to express our appreciation for the cooperation and courtesies extended to us during this audit.

Attachment

C: Claudia Puig, Chair, FIU Board of Trustees
Gerald C. Grant Jr., Chair, FIU Board of Trustees Finance and Audit Committee
FIU Board of Trustees Finance & Audit Committee Members
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost and Executive Vice President
Javier I. Marques, Chief of Staff, Office of the President
Kristina Raattama, General Counsel
Alexander D. Casas, Chief of Police
Barbara Manzano, Assistant Vice Provost, University Planning and Finance

TABLE OF CONTENTS

OBJECTIVES, SCOPE AND METHODOLOGY

Pursuant to our approved annual plan, we have completed an audit of University Building Access Controls. The primary objective of our audit was to determine if policies and procedures related to building access controls were adequate and effective. This included the evaluation of controls in place to prevent unauthorized access and safeguard resources.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing,* and included tests of the access control records and other auditing procedures, as we considered necessary under the circumstances.

During the audit, we evaluated the adequacy of the access controls over University buildings and facilities requiring protection (e.g., labs, utilities, and data centers), including the process for requesting and removing faculty, student and staff access privileges. This audit, however, did not include access controls over museums and student housing, which was already covered in previous audits.

We reviewed University policies and procedures, Florida statutes and regulations, observed current practices and processing techniques, interviewed responsible personnel, reviewed supporting documentation, and tested selected transactions. Sample sizes and transactions selected for testing were determined on a judgmental basis. Audit fieldwork was conducted from March to April 2015 and July to August 2015.

While this was the first internal audit of University Building Access Controls, there were prior internal audit recommendations related to the scope and objectives of this audit requiring follow-up. Our internal audit report on the PantherCARD Financial, Operational, and Information Systems Controls, issued on August 8, 2011 (Report No. 11/12-02) contained four recommendations, which were addressed to the Key Control Section of the Facilities Management Department. The results of our follow-up testing related to those previous recommendations are covered in section five of this report on page 22.

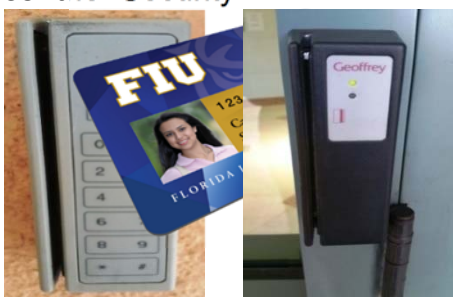
BACKGROUND

Pursuant to Florida Board of Governors Regulation §1.001(3)(l), *University Board of Trustees Powers and Duties, University Administration and Oversight,* each board of trustees shall be responsible for campus safety … to include safety and security measures for university personnel, students, and campus visitors. In furtherance of the BOG regulation, FIU established Procedure §520.005a, which establishes the Facilities Management Department as the central point for the issuance, maintenance and secured storage of all types of software, hardware and access mechanisms used on interior and exterior doorways for all campus buildings and facilities. The Key Control Section (Key Control) of the Facilities Management Department is responsible for implementing the procedure. They maintain all doors, exit devices, handicap openers, and all related hardware for the entire campus. This includes electronic locks and controlled access.

Key Control plays a significant role for access controls at the University's two major campuses, Modesto A. Maidique Campus (MMC) and Biscayne Bay Campus (BBC), and various other locations. There are 87 buildings at MMC containing 16,197 rooms and 18 buildings at BBC that have 2,201 rooms. At any given time, any of 54,000 students, 11,000 employees, and numerous others visit our facilities.

The primary access control to University buildings (both exterior and interior) is provided by a manual key system and/or a "FIU One Card" electronic access system. Working with the building users, Key Control determines the keying and issuance of keys. In addition to simple door keys, there are also various types of master keys. The holder of a key to any University facility assumes responsibility for the safekeeping of the key and control over its use.

For the electronic access system, the University uses the Security Management System (SMS), which allows the FIU One Card to be used as the means of access. The online electronic access technology replaces traditional keys with an electronic door strike that is hard-wired and networked into the current information technology infrastructure to allow for remote communication.

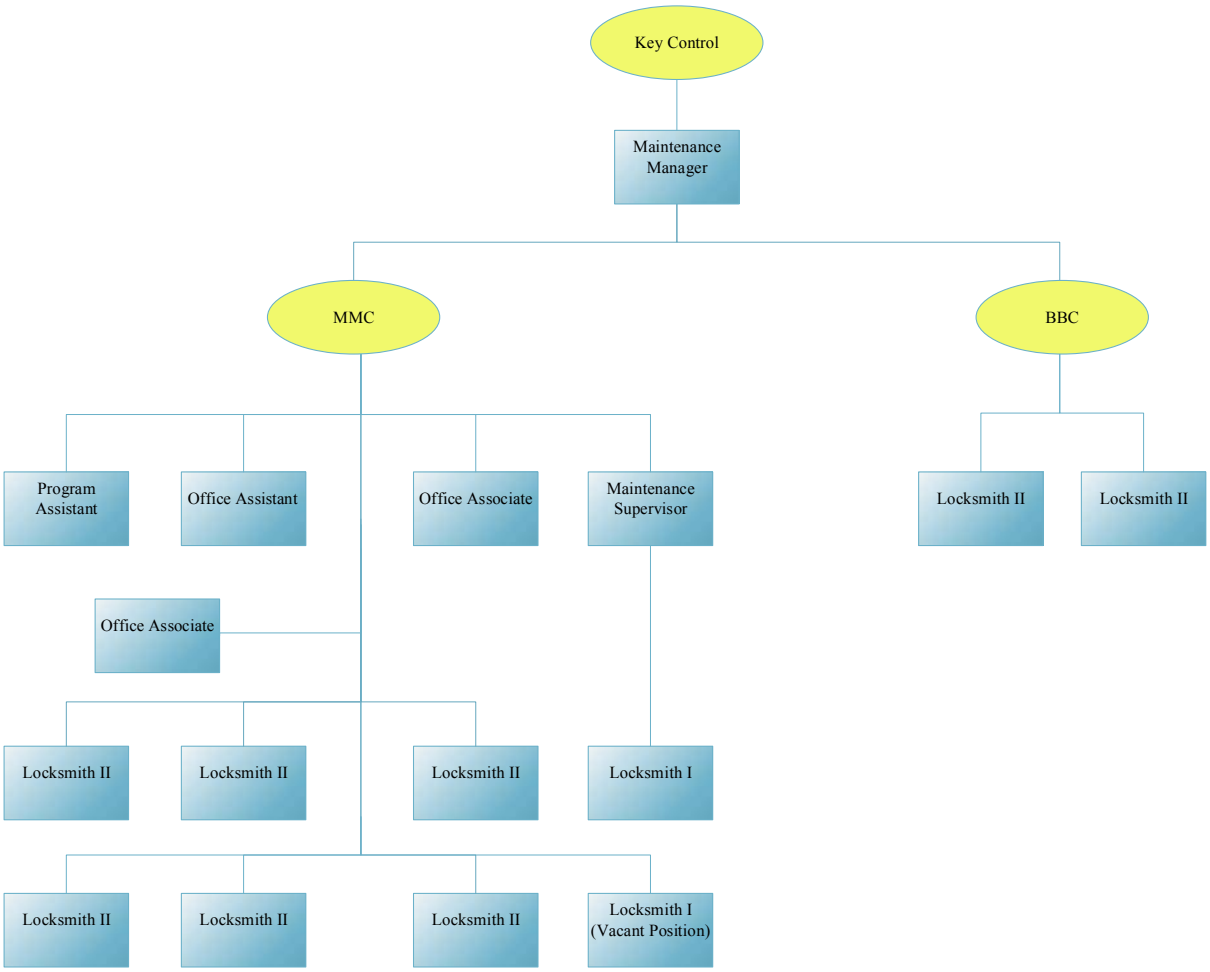


The University also uses an offline electronic access door lock (prior SMS version), which is a stand-alone unit that cannot be programmed remotely and does not have remote lockdown capability. The offline electronic lock stores all access history and is maintained in the lock's memory, which requires periodic visits to download/upload information and for battery replacement.

Key Control is accountable for ensuring that specific access is activated based on proper authorization by the requesting department and deactivated upon employee separation or change in assignment. In order to improve request completion times, Key Control is delegating the responsibility of building access privileges to specific colleges and departments.

Financial and Personnel Information

For the fiscal year 2015-16, Key Control budgeted $802,005 for payroll related expenses for 16 full-time positions and $115,000 for other operational expenses. The Key Control's organization chart is illustrated below.



FINDINGS AND RECOMMENDATIONS

Overall, our audit disclosed that policies and procedures related to building access controls are inadequate. Controls to prevent unauthorized access, safeguard resources, and promote safety need significant improvement in all of the topical areas reviewed. This will require a significant and timely collaborative effort by cognizant officials throughout the University. Our overall evaluation of internal controls is summarized below.

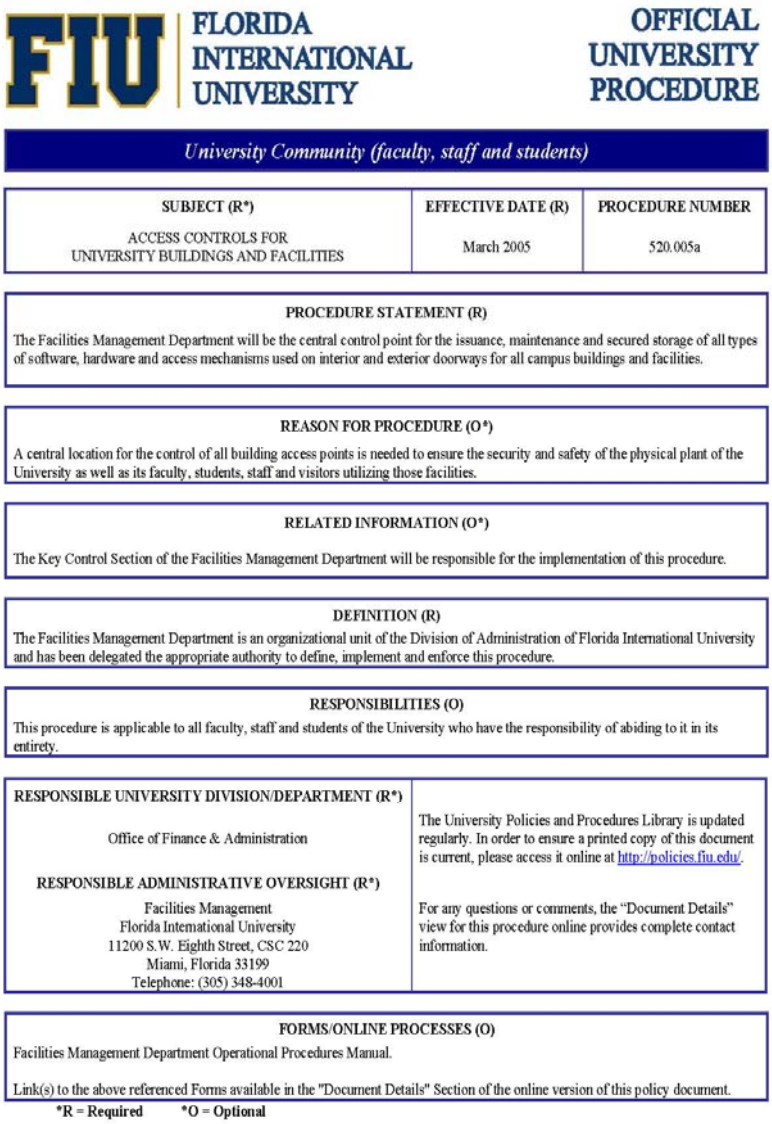
INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**X**	
Policy & Procedures Compliance			**X**
Effect			**X**
Information Risk			**X**
External Risk			**X**
INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	**Effective**	**Opportunities exist to improve effectiveness.**	**Do not exist or are not reliable.**
Policy & Procedures Compliance	**Non-compliance issues are minor.**	**Non-compliance Issues may be systemic.**	**Non-compliance issues are pervasive or have severe consequences or policy & procedures are significantly lacking.**
Effect	**Not likely to impact operations or program outcomes.**	**Impact on outcomes contained.**	**Negative impact on outcomes.**
Information Risk	**Information systems are reliable.**	**Data systems are mostly accurate but can be improved.**	**Systems produce incomplete or inaccurate data, which may cause inappropriate financial and operational decisions.**
External Risk	**None or low**	**Medium**	**High**

Our findings and recommendations follow:

1. Policies and Procedures

According to University Procedure No. 520.005a, *Access Controls for University Buildings and Facilities*, a central location for the control of all building access points is needed to ensure the security and safety of the physical plant of the University as well as its faculty, students, staff and visitors utilizing those facilities. Key Control is the central focal point for the control of all building access points that ensure the security and safety at the University.

We reviewed the procedure and other relevant information posted on the Facilities Management Department's website, and interviewed accountable personnel to determine if the current building access procedures are adequate and effective to prevent unauthorized access and safeguard resources. Our review disclosed that a more comprehensive policy and more detailed procedures for building access controls would serve to minimize risks and maximize the protection of the University's physical plant and personnel.



FIU FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

University Community (faculty, staff and students)

SUBJECT (R*)	EFFECTIVE DATE (R)	PROCEDURE NUMBER
ACCESS CONTROLS FOR UNIVERSITY BUILDINGS AND FACILITIES	March 2005	520.005a

PROCEDURE STATEMENT (R)

The Facilities Management Department will be the central control point for the issuance, maintenance and secured storage of all types of software, hardware and access mechanisms used on interior and exterior doorways for all campus buildings and facilities.

REASON FOR PROCEDURE (O*)

A central location for the control of all building access points is needed to ensure the security and safety of the physical plant of the University as well as its faculty, students, staff and visitors utilizing those facilities.

RELATED INFORMATION (O*)

The Key Control Section of the Facilities Management Department will be responsible for the implementation of this procedure.

DEFINITION (R)

The Facilities Management Department is an organizational unit of the Division of Administration of Florida International University and has been delegated the appropriate authority to define, implement and enforce this procedure.

RESPONSIBILITIES (O)

This procedure is applicable to all faculty, staff and students of the University who have the responsibility of abiding to it in its entirety.

RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT (R*)	
Office of Finance & Administration	The University Policies and Procedures Library is updated regularly. In order to ensure a printed copy of this document is current, please access it online at http://policies.fiu.edu/.
RESPONSIBLE ADMINISTRATIVE OVERSIGHT (R*) Facilities Management Florida International University 11200 S.W. Eighth Street, CSC 220 Miami, Florida 33199 Telephone: (305) 348-4001	For any questions or comments, the "Document Details" view for this procedure online provides complete contact information.

FORMS/ONLINE PROCESSES (O)

Facilities Management Department Operational Procedures Manual.

Link(s) to the above referenced Forms available in the "Document Details" Section of the online version of this policy document.

*R = Required *O = Optional

- Specific roles and responsibilities for Key Control and University departments except for those departments that have delegated authority to manage the electronic access to their areas. For instance, the current

procedure does not address individual colleges/departments' responsibilities for the control of key or electronic card access.

- Types of the access level to be granted to various faculty, staff, and contractors. For instance, who or which departments should receive Great Grand Master Keys (GGMK), Building Master Keys, and/or Super Electronic Access, etc., and under what circumstances.

- Requesting and granting electronic access.

- Authorizing high-level access such as GGMK and Building Master Key by respective Vice President or Dean.

- Periodic physical inventories of keys issued.

- Replacement fee for lost or stolen Great Grand Master Keys.

- Granting and removing the key and/or electronic access for outside vendors.

- Proscribed activities such as duplication of keys, transfer of keys without authorization, or circumventing security, for example by propping doors open.

- Periodic building lock down testing.

We reviewed policies and/or procedures at four other universities, University of Florida, Florida State University, University of Central Florida and University of Miami. All of them have comprehensive policies on the issuance of keys and electronic access. Their policies clearly delineate the roles and responsibilities of their key control units and their individual colleges/departments, what types of access are to be granted, who is responsible for conducting key inventories, and what records should be kept.

The University's current procedure on *Access Controls for University Buildings and Facilities* (No. 520.005a), addresses the reason for the procedure and who is responsible for implementing the procedure, but does not provide guidance to colleges/departments on how to manage their buildings/facilities access control. In addition, Key Control does not have written procedures, typically found in an operations manual to assist them in implementing the procedure.

There is a lack of clarity as to what actions should or should not be taken under any given set of circumstances. For example, when two Great Grand Master Keys were reported as lost, there was no documentary evidence of any actions taken. A procedure might prescribe the necessity of conducting an investigation and performing a risk assessment to justify not rekeying locks, and/or what are the ramifications to the departments or employees who lost their key.

The safety and security of the University's physical space and assets is a shared responsibility of all members of the University community. Therefore, having a comprehensive building access control policy and/or procedures for the University community and developing an operations manual for Key Control will minimize risks and maximize the protection of the University's buildings and physical assets.

Recommendations

The Facilities Management Department should:	
1.1	Work with the University community, especially the Police department, to develop a comprehensive policy and/or procedures for buildings/facilities access controls.
1.2	Direct Key Control to develop a comprehensive operations manual.

Management Response/Action Plan:

1.1 FMD concurs. FMD will coordinate the creation of a committee to develop new policy and procedures. University representation will include the Police Department, Human Resources, Legal and others as appropriate.

Implementation date: April 30, 2016

1.2 FMD concurs. Key Control Department will develop an operations manual. While the operations manual will be dependent on developing the comprehensive policies & procedures referenced in Recommendation 1.1, FMD will concurrently work with the committee in drafting the operations manual.

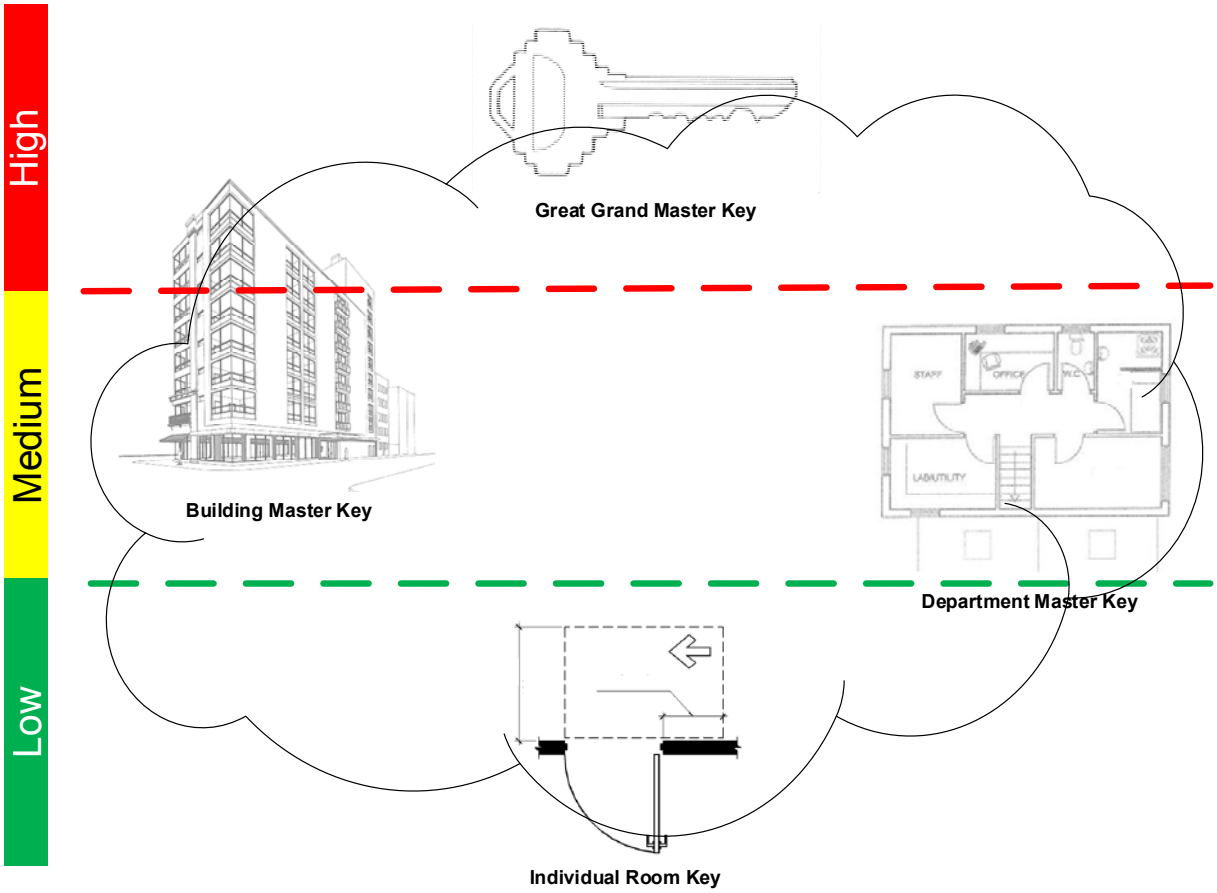
Implementation date: June 30, 2016

2. Key Access Controls

a) Issuing Keys

In order to obtain a key for specific buildings/rooms' access, Facilities Management developed an online Key Request form. The departments fill out information such as employee name, Panther ID, department, building, room and key type to create the "Key Request Confirmation Page". The confirmation is then printed, signed by the employee, approved by the respective department head/supervisor, and delivered to Key Control. Key Control verifies the department head/supervisor's signature with Key Authorization Signature forms on file, and issues a key to the respective employee.

The diagram below shows the type of keys with their associated risk for most common areas.



Great Grand Master Key: operates all locks in all buildings on campus
Building Master Key: operates all locks within a building
Department Master Key (Sub-master or Floor-master): operates all locks within a department
Individual Room Key: operates a specific room

(Figure 1 - Keys with Associated Risk)

The Key Request Confirmation Page states in part: 1) the key holder is personally accountable for all university keys issued to them; 2) all building master keys must be co-signed by the Assistant Vice President [presently Associate Vice President] of Facilities Management; and 3) all department master keys can be co-signed by either the Assistant Vice President or the Associate Director [presently Executive Director] of Facilities Management.

We selected 64 individuals (62 active employees and 2 contractors) to determine if the keys issued to them were in accordance with the procedure established by Facilities Management. They were issued 269 keys to such areas as the Academic Health Center, the Labor Center, Athletics, the Campus Support Complex, and the PG5 Market Station.

Our review disclosed that all of keys issued aligned to their official work location; however, the following conditions were noted:

- For three keys issued to two employees, the Key Request Confirmation Page documentation was unavailable.

- The Key Authorization Signature form was not maintained to support three keys issued to one employee. According to Key Control, they typically destroyed the completed Key Authorization Signature forms when blank forms are updated because of departmental head/supervisor changes.

- Keys were issued to two vendors (a Construction Manager and the Panther Dining vendor) without a written approval from the respective departments (Facilities Management and Business Services) which manage these vendors. According to Key Control, the University Project Manager from Facilities Management sent them an email for the Construction Manager's request for keys. However, the email was not available for review. For the Panther Dining vendor, ARAMARK, Key Control indicated they are treated as a University department, since they stay on campus for a long-term basis.

- One building master key for a Construction Manager and two department master keys, one for a student intern and the other for a vendor, were issued without obtaining approval from the Associate VP of Facilities and/or the Executive Director of Facilities. The department master key issued to the student intern was approved by the Key Control Maintenance Manager. He stated that he and his supervisor, an Assistant Director of Physical Plant, are allowed to approve department master keys, but that is contrary to the procedure outlined on the Key Request Confirmation Page.

b) Returning Keys

Keys issued to terminated or transferred employees were not always returned to Key Control as required. The Key Request Confirmation Page states in part that: 1) it is the key holder's responsibility to return all keys to Key Control; 2) loss or failure to return an assigned key may subject the key holder to a replacement fee; 3) the University reserves the right to charge the key holder for any rekeying due to loss of an assigned key; 4) if the key holder is terminated or resigns, fees must still be collected; 5) the University reserves the right to charge the department for lost or stolen keys or cylinder re-key to doors if not collected from key holder.

Please print in Landscape

Facilities Management Key Request Confirmation Page

Last Name **First Name** **MI**

FIU ID # **Department**

Relationship **Student Expiration Date** **Telephone**

Key Control Use Only

Building Initials	Room	Key Type	Key #	Ret. Date	Signature	Initials

University Key Policy

1) The key holder is personally accountable for all university keys issued to them.
2) It is the key holder's responsibility to return all keys to Key Control.
3) All Building Master's must be co-signed by the Assistant Vice President of Facilities Management. All Department Masters can be co-signed by either the Assistant Vice President or the Associate Director of Facilities Management.
4) University keys may not be exchanged or loaned
5) Loss or failure to return an assigned key may subject the key holder to a replacement fee.
6) The University reserves the right to charge the key holder for any rekeying due to loss of an assigned key.
7) **Lost or stolen keys** must be reported to FIU Public Safety within 24 hours.
8) Lost or stolen keys will result in a replacement charge. **$50.00 individuals, $250.00 Department Masters, $500.00 Building Masters.**
9) All damaged keys must be returned to Key Control for replacement.
10) If key holder is terminated or resigns, fees must still be collected.
11) The University reserves the right to charge the department for lost or stolen keys or cylinder re-key to doors if not collected from key holder.

I have read the above statement and agree to abide by it.

Key Holder's Signature Date

Department Head/Supervisor Name Department Head/Supervisor Signature Date

Thank You for submitting your information.
Please provide the appropriate signatures and deliver this confirmation page to W3 100 for UP or So3 208 for BBC.
Key Control hours of operation are 8:30am to 4:30pm M-F.

To determine if keys were properly returned to Key Control, we tested records for 19 employees (14 terminated and 5 transferred employees) who were issued 63 keys. Our test disclosed that 47 of the 63 keys (75%) were not returned to Key Control. These included 16 master keys for employees terminated or transferred between November 2000 and February 2015.

According to Key Control, it is difficult to ensure that all keys are being returned by terminated or transferred employees in the absence of cooperation from departments. Although the department's supervisor is responsible for completion of a Separation from Employment/Transfer Clearance form, which includes the employees' acknowledgement that the key(s) were returned, the process appears to be awkward and not working as intended.

Since periodic physical inventories or reconciliations are not performed, it is not evident how many unreturned or lost/missing keys are in circulation. This increases the risk of inappropriate access to the University buildings/facilities.

Recommendations

The Facilities Management Department should:	
2.1	Ensure that Key Control strengthen its key issuing process including record keeping practices and record retention.
2.2	Work with the individual departments and Human Resources to strengthen the key return process.

Management Response/Action Plan:

2.1 FMD concurs. FMD will develop an automated on-line access request process (e-process) for both hard keys and electronic card access. This e-process with e-signature and full audit capability will be developed to replace the current paper record process.

Implementation date: June 30, 2016

2.2 FMD concurs. The electronic process referenced in Recommendation 2.1 will include key returns, in accordance with newly developed policy and procedures from Recommendation 1.1.

Implementation date: June 30, 2016

3. Electronic Access Controls

a) Granting Electronic Access

Key Control uses the Security Management System (SMS) for the management of electronic access. According to the Key Control Maintenance Manager, Key Control grants electronic access after receiving an email from the department requesting the access to specific areas. Some departments are allowed to manage their own areas. However, there is no written procedure for requesting and granting electronic access to University buildings/rooms, as mentioned in the previous section of this report.

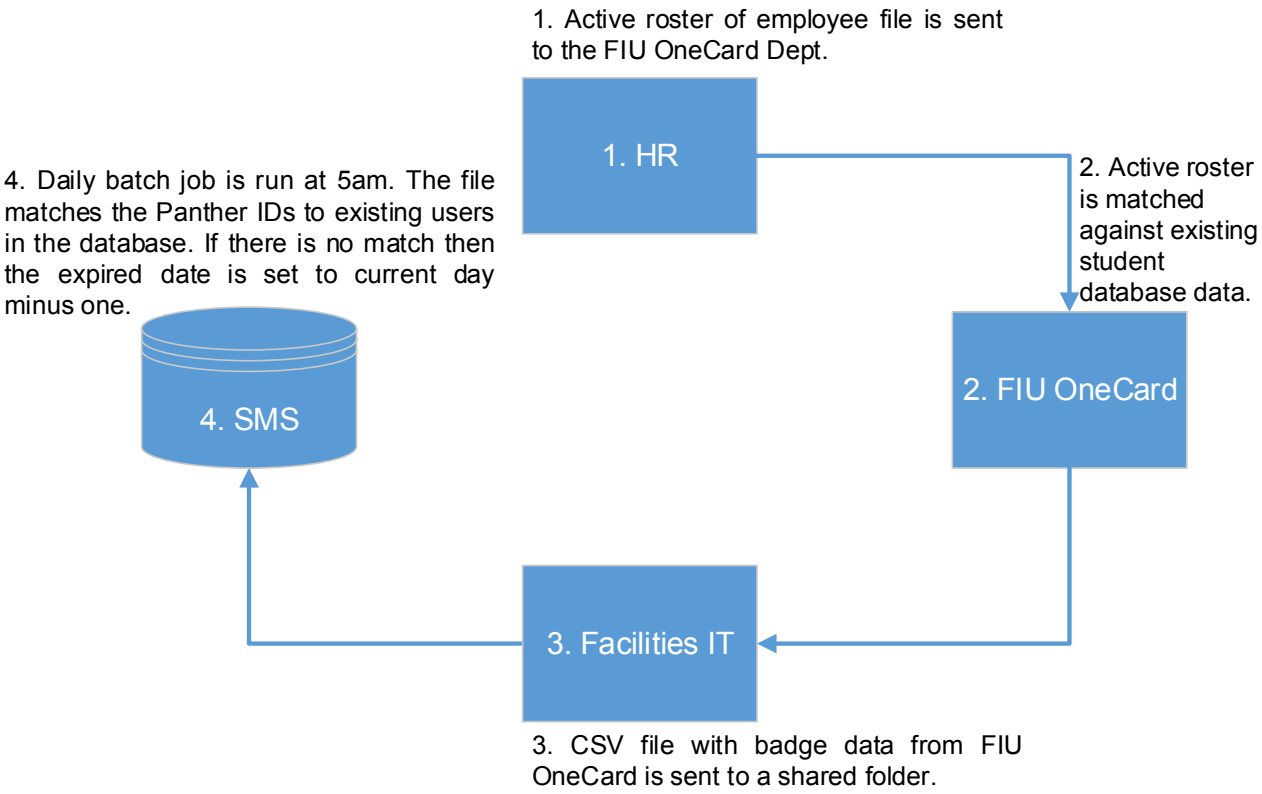
To determine if the electronic access was granted to individuals with adequate supporting documents (email requests), we selected 21 individuals including 5 contractors who had access to specific University buildings/rooms for testing. Our test disclosed that Key Control was unable to provide supporting documents (email requests) for 17 of the 21 individuals tested. According to Key Control, the request emails are archived in their shared drive by the date requested. The current process, however, is ineffective in identifying user access, which leaves the University unnecessarily vulnerable.

In addition, the access expiration date for the selected 21 individuals was December 31, 2199. According to Key Control, this access expiration date is a default setting granted for all users, since employee dates of departure are usually indeterminate. However, we identified 71 contractors with the default expiration date. For example, a construction manager's access was granted through 2199, even though the construction project was completed in 2013. Without an expiration date that is aligned to the contract period, it may lead to inappropriate building access.

We also found that some employees have access to areas that do not pertain to their job responsibilities. For example, a biology professor and a maintenance support worker at BBC had access to the AHC4 IT room and MMC Central Utilities, respectively. Two employees in the Controller's Office had electronic access to the Office of Internal Audit (OIA). When we discussed this with one of the employees, she stated that she had no knowledge of her access to the OIA and never requested it.

b) Revoking Electronic Access

According to Key Control, a process to remove the terminated employees' access is automatically performed on a daily basis. Figure 2 illustrates the current automated process to disable terminated users building/room access.



(Figure 2 – Terminated Employees' Automatic Deactivation Process)

Our testing revealed that the process was not working as intended. As of March 2015, there were 63,195 active user accounts in the SMS application. Our review of these accounts disclosed that there were 5,053 terminated users and 2,200 users without a corresponding Panther ID.

To determine if the terminated users had access to buildings/rooms, we selected and examined a sample of 300 terminated users. Of the 300 terminated users, 203 (68%) users' access was not deactivated, although their termination dates ranged from one month to 10 years ago. In addition, out of the 203 users, we:

- Identified 70 having offline access, which allows keypad access using a code, even if they returned their FIU One Card; and
- Examined a Separation from Employment/Transfer Clearance form for 21 users and found that 9 did not return their card; thus, they still had access to buildings/rooms.

In order to determine if the users without a Panther ID had access to buildings/rooms, we reviewed 250 users and identified 64 as terminated employees. Our further review of these 64 terminated employees disclosed that 31 (48%) still had access to their prior work locations, including wet labs containing chemicals or biohazardous materials.

We also selected eight different risk areas from Central Utilities, AHC4, and PC buildings to determine if transferred employees had access to their prior work locations. We reviewed all users who had access to these selected areas and determined that six employees were transferred to other departments. Our test of the six transferred employees' access disclosed that all of them still had access to their prior locations, although their transfer dates ranged from 3 months to 4.5 years ago.

Additionally, we selected 162 system operators from 72 departments, who managed their area's electronic access, to determine if their access is still valid. Our review disclosed that out of the 162 operators, six were terminated, three were transferred to other departments, and one retired. Although the access was removed from all of the terminated operators, one retired and two transferred operators still had access to their prior work location. The employee retired on August 4, 2012, while the other two employees transferred on July 13, 2013 and January 3, 2015, respectively.

Not revoking the access of terminated and/or transferred employees increases the University's security risk.

Recommendations

The Facilities Management Department should:	
3.1	Ensure that Key Control strengthen its process for granting and revoking electronic access.
3.2	Ensure that Key Control work with Human Resources to remove/update access for all terminated or transferred employees.

Management Response/Action Plan:

3.1 FMD concurs. The current electronic process will be reevaluated and changes will be made to strengthen the system and reduce/eliminate the anomalies that were referenced in the audit report, in accordance with newly developed policy and procedures from Recommendation 1.1.

Implementation date: June 30, 2016

3.2 FMD concurs. As part of the new e-process, FMD will receive a continuous feed of information from HR/Peoplesoft about employee status. This information will be incorporated into an automated workflow to take action and notify decision makers.

Implementation date: June 30, 2016

4. Oversight/Management of Building Access Controls

Key Control is the central focal point for the control of all building access points that ensure the security and safety at the University. It uses the KeyTrail software and Security Management System (SMS) to manage key and electronic access. Key Control also developed a *Key Control Acceptable Use Agreement*, which allows specific colleges/departments to manage their own area's electronic access.

During the audit, we observed the current process for controlling and monitoring key and electronic access, and determined that the process needs improvement. Detail follow:

- The data stored in KeyTrail contained unencrypted employees' social security number (SSN). For example, for 126 of the 738 employees who were recorded as having master keys in the KeyTrail system, SSNs were still being used for identification purposes instead of their Panther ID number. The number of records using employee SSNs are likely much greater when taking into consideration other employees have individual room keys. It appears that records using SSNs were not converted to Panther IDs for those employees who received keys prior to implementation of PantherSoft Solutions in 2004.

  According to University IT Security Policy, departments or units that collect or maintain SSNs must abide by the requirements of the University Data Stewardship Procedure, which requires highly sensitive data stored in electronic format to be encrypted. It should also be noted that our testing revealed that the KeyTrail database had erroneous entries such as incorrect Panther ID numbers and duplicate key tag entries.

- Our review of the KeyTrail application user privileges disclosed that all 13 system users have administrator access, which includes the ability to add, delete, and update user accounts. There is even one generically-named administrator account that can be used to make unauthorized changes without being traced to an individual. Additionally, passwords are not encrypted and appear to be iteratively assigned, which increases the risk that a user could log in with another's credentials.

- Periodic physical inventories of keys have never been performed by Key Control or other departments to account for the keys they have issued. Therefore, management does not know exactly how many keys are missing or stolen when they are not reported by key holders or departments. For instance, our review of Great Grand Master Keys and Building Master Keys for four buildings at MMC disclosed that there were keys that were unaccounted for as noted in the following table:

Type of Key	Selected Building	Total Number of GGMK or Building Master Keys				
		Total	Assigned to Employees	Reported as Lost or Stolen	Kept in Key Control	Unaccounted For
GGMK	All	19	16	2	1	0
BMK	CP	15	2	1	9	3
BMK	AHC1	23	8	0	3	12
BMK	AHC3	10	7	1	1	1
BMK	AHC4	7	3	0	2	2

GGMK: Great Grand Master Key
BMK: Building Master Key
CP: Chemistry & Physics
AHC: Academic Health Center

According to Key Control, it is difficult to manage keys in the absence of cooperation from the University community and a strong key policy for securing keys and charging for lost or stolen keys. They believe that key holders who may be held financially responsible for key replacement might not be reporting lost keys. Therefore, without periodic accounting for the keys issued and cooperation from the departments, Key Control is unable to determine how many keys and what type of keys are missing.

- Most keys used at BBC including master keys can be easily duplicated, which creates a security risk. According to Key Control, more than 80% of the BBC buildings are using a type of key that can be easily duplicated at any locksmith store. During the audit, we were informed that due to insufficient budget, only one building, the Marine Science Building, some areas in AC1, and Telecommunication rooms at BBC were converted to the more secure locking system currently used at MMC.

- Key Control at BBC could not provide data on how many keys, including Great Grand Master, Building Master, and Department Master keys were issued. The Key Control at the BBC had been working without having access to their key database since 2010. Because they thought the data was lost, they began reconstructing key information onto an Excel spreadsheet. However, we learned from the Facilities IT Director that the key data was in fact never lost but was kept in a FMD network shared drive that Key Control was unaware of.

- We observed that many keys, not traceable to key records, were kept on an office desk at BBC Key Control. According to Key Control personnel, many of these keys were collected, reassigned, stored by departments without their knowledge, and later returned. Since Key Control maintained incomplete key information on their Excel spreadsheet and had no access to the key database, it was difficult to identify to whom these keys were originally assigned.

- The departments/colleges with delegated authority from Key Control to manage their area's electronic access did not fulfill their roles and responsibilities as required by the *Key Control Acceptable Use Agreement*. We selected 35 System Operators from 72 departments and surveyed them about their access control experiences. Eighteen of them responded to our survey and provided the following noteworthy information:

    - Nine Operators did not run "unauthorized access & history reports" to review potential unauthorized access to their areas. One indicated that he was not authorized to run the report and the other did not know how to run the report because he was not trained.

    - Fourteen Operators did not run a status report for existing or terminated card users every semester to be submitted to Key Control. The remaining four Operators ran the report, but only one Operator submitted the results to Key Control.

    - Six Operators did not maintain records to support granting and terminating access to their location.

    - Eight Operators indicated that they did not receive adequate guidance or training from Key Control. Two of the eight noted that they never received training.

- For those departments that have no delegated authority, Key Control manages the electronic access to their areas. However, Key Control did not review status audit reports and unauthorized access & history reports, which assists them in identifying invalid and potential unauthorized access to the areas.

- Our test of Security Management System (SMS) user accounts identified:

    - Six operator generic accounts without expiration dates and two generic accounts (generic ID card and code) issued as "temporary officers" in the Police Department, providing access to all University buildings/facilities,

were not assigned to specific individuals, thus, the user identity for these accounts cannot be tracked.

- One administrator system account was issued to a contractor who supports the SMS system.

- Two generic ID cards were issued to a Refrigeration Mechanic and one generic ID card was issued to a Custodian. These generic ID cards were not deactivated although the access was granted through their FIU One Card.

According to Key Control, generic user accounts were created for testing and should have been disabled. Administrator accounts can be used to make major changes to the system and applications. The Administrator accounts have the ability to access all data in the system, and can use all features of the applications, as well as perform any required administrative or corrective action.

We also observed that Key Control had no periodic tracking system to account for how many generic cards were received, issued, and on hand. We were informed that blank generic ID cards are issued to contractors with an expiration date for their contracted work. However, we noted that generic ID cards were also issued to employees/departments.

Finally, Key Control did not always document periodic building lock-down test results, although they indicated that tests were performed annually with the exception of last year. No documentation, however, was provided except for 3 buildings in late 2012 and 5 buildings in early 2013. Building lock-down tests should be performed periodically and documented to ensure that building occupants are adequately protected in the case of an emergency.

Recommendations

The Facilities Management Department should:	
4.1	Ensure that Key Control: a) remove sensitive data from its database and b) maintain a complete key database at BBC and resolve all key related accountability issues.
4.2	Develop procedures to perform periodic physical inventories of keys, especially master keys.
4.3	Determine whether the BBC lock system should be upgraded.

4.4	Provide guidance and/or training to all individuals who have been delegated facilities access control responsibilities.
4.5	Establish a process to periodically validate electronic access privileges.
4.6	Disable generic user accounts; reduce administrator privileges based on least privileged principles; and limit temporary administrator system account to contractor on an as need period of time.
4.7	Ensure that Key Control maintain documentation for building lock-down test results and any corrective actions taken.

Management Response/Action Plan:

4.1 a) FMD concurs. FMD will prioritize removal of sensitive data and make it a top priority.

Implementation date: February 29, 2016

b) FMD concurs. FMD will develop the electronic system to address accountability issues. The new e-process will include BBC.

Implementation date: June 30, 2016

4.2 FMD concurs. FMD will develop procedures to perform inventories. The intent is to inventory master keys annually and other keys on a random, spot-check basis.

Implementation date: June 30, 2016

4.3 FMD concurs. Estimated cost is $180,000. A budget request will be made for FY 2016-17. Implementation is projected to require a full year after funding.

Implementation date: Pending

4.4 FMD concurs. FMD will strengthen the current training regimen, including electronic on line records of training.

Implementation date: June 29, 2016

4.5 FMD concurs. FMD will periodically validate access for only those users who do not have an access administrator, in accordance with newly developed policy and procedures from Recommendation 1.1

Implementation date: June 30, 2016

4.6 FMD concurs. Generic user accounts have been removed. Temporary cards will be issued to external third parties once the Person of interest (POI) process is completed with specific expiration dates. Administrator rights will be limited to key control electronic access managers. Temporary administrator rights for testing purposes will be granted only for one-day duration.

Implementation date: Immediately

4.7 FMD concurs with comment. E-mail correspondence documents past lockdown tests and corrective actions. Documentation will be strengthened using the Maximo work order system. Lock downs will also be addressed in the University policy.

Implementation date: June 30, 2016

5. Implementation of Prior Audit Recommendations

One prior audit report on the PantherCARD Financial, Operational, and Information Systems Controls, issued on August 8, 2011 (Report No. 11/12-02) contained four recommendations, which were addressed to Key Control. Our current test of the four recommendations disclosed that:

- two were satisfactorily implemented; and
- two were partially implemented.

Below are our test results for each recommendation:

Recommendation		Fully Implemented	Partially Implemented	Not Implemented
PantherCARD Building Access				
12.1	Ensure that delegated colleges follow the required process. (The process required the documentation of username, Panther ID, and location.)		✓	
12.2	Require delegated colleges and departments to sign the Key Control Acceptable Use Procedure statement.	✓		
12.3	Ensure delegates perform acceptable access provisioning and de-provisioning procedures by adequately documenting delegated roles and responsibilities within the Key Control Acceptable Use Procedure document.	✓		
12.4	Work with Human Resources to implement procedures to revoke PantherCARD access to premises, buildings, and areas in a timely and accurate manner.		✓	

The following are our current observations for the recommendations determined to be not fully implemented.

12.1 Ensure that delegated colleges follow the required process.

This recommendation was previously reported as fully implemented by management. In order to implement the recommendation, Key Control reported that they would monitor all system operators through quarterly audit reports generated by the SMS software. However, as previously discussed earlier in this report, Key Control is not monitoring all system operators through quarterly audit reports.

12.4 Work with Human Resources to implement procedures to revoke PantherCARD access to premises, buildings, and areas in a timely and accurate manner.

This recommendation was previously reported as fully implemented by management; however, our testing revealed that the access for terminated employees was not always revoked. Our test of 300 terminated users disclosed that 203 (68%) users' access was not revoked. (See our detail testing at the Revoking Electronic Access section of this report.)

Recommendation

The Facilities Management Department should:	
5.1	Take steps to fully implement prior recommendations.

Management Response/Action Plan:

5.1 FMD concurs. Policy and procedures from Recommendation 1.1 will further facilitate the implementation of prior recommendations.

Implementation date: June 30, 2016